



Coverity® Announces the State of Open Source Software Integrity

Releases 2009 Coverity Scan Open Source Report

Coverity, the software integrity leader, today released the 2009 Coverity Scan Open Source Report. This report is the result of the largest public-private sector research project focused on open source software integrity. Originally initiated with the U.S. Department of Homeland Security, the 2009 Coverity Scan Open Source Report details the findings from analysing more than 11 billion lines of open source code from 280 open source projects over the last three years. The Coverity open source integrity report is an objective presentation of open source code quality and defect data collected from the Coverity Scan service. The report findings provide a unique opportunity for the business industry to examine coding and software integrity trends from some of the worlds most well-used and popular open source packages, including Firefox, Linux, PHP, Ruby and Samba. Some highlights of the report findings include: Overall integrity, quality and security of open source software are improving. The Coverity Scan service measured a 16 percent reduction in static analysis defect density over the past three years among participating projects. Open source developers are actively improving software. Since 2006, more than 11,200 defects in open source programs have been eliminated as a result of using the Coverity Scan service. Total developer support has increased with more than 180 projects having active developers scanning and fixing software defects discovered by Scan. Projects continue to advance up Coverity Certified Integrity Rungs from year to year. In 2009, the number of Rung 1 certified projects increased 32 percent from 2008 and doubled on Rung 2 in the same time period. OpenPAM, Ruby, Samba and tor are the first projects to begin Coverity Integrity Rung 3 certification. Rungs are certification levels indicating high-integrity open source software. Most common defect types are holding steady. The most common defect types across participating open source projects are still NULL Pointers, resource leaks and unintentional ignored expressions. High-integrity open source software is critical, especially given Gartners estimate that at least 80 percent of commercial software will contain open source code by 2012, 1 said David Maxwell, Coverity open source strategist. Coverity would like to thank all the open source teams and developers who participate in Coverity Scan. This report could not have happened without their support. Specifically, we applaud the OpenPAM, Ruby, Samba and tor teams for embarking on their Coverity Integrity Rung 3 certification. The 2009 Coverity Scan Open Source Report includes the following topics: Introduction to static analysis; Open source projects participating in Coverity Scan; Overall code improvements by participating projects; Projects with most improved quality and how it was achieved; Most commonly found defects; Function length and defect density; Complexity metrics and defect density. The Coverity Scan service began as a public-private research partnership with the U.S. Department of Homeland Security to harden the integrity of open source code, said Andy Chou, chief scientist and co-founder of Coverity. The Coverity Scan service is a key pillar of our strategy to help open source and commercial developers to continually improve the integrity of all software. Powering the integrity Scan service is Coverity Static Analysis, the industrys leading static analysis product. In February 2009, Coverity also published application architecture data for more than 2,500 popular open source software projects and provides this information as part of the free service to the open source community. For more information about Coverity Scan and to download the 2009 Coverity Scan Open Source Report, visit <http://www.coverity.com/scan>. To hear what open source project leaders have to say about software integrity, go to <http://blog.coverity.com>. Coverity will be hosting a free webinar to delve deeper into the findings from the 2009 Coverity Scan Open Source Report. To register for the event, visit <http://www2.coverity.com/1/584/2009-09-09/ESBU7>. About Coverity Coverity (www.coverity.com), the software integrity leader, is the trusted standard for companies that have a zero-tolerance policy for software failures, defects and security breaches. Coverity's award-winning portfolio of software integrity products identifies critical defects to prevent software quality and security problems throughout the application lifecycle. More than 100,000 developers and 600 companies rely on Coverity to help them deliver high-integrity software. Coverity is a privately held company headquartered in San Francisco. Coverity is a registered trademark of Coverity, Inc. All other company and product names are the property of their respective owners. (1) Gartner. Gartner Highlights Key Predictions for IT Organisations and Users in 2008 and Beyond. <http://www.gartner.com/it/page.jsp?id=593207>.

Contacts

Ramzi Kattan
02 9687 1880
mailto: ramzi.kattan@emlogic.com.au